WEST RAND
DISTRICT MUNICIPALITY

RISK MANAGEMENT POLICY FRAMEWORK

TABLE OF CONTENTS

SECTION 1: INTERPRETATION AND INTRODUCTION

1.1 DEFINITIONS

In this Policy Framework, unless the context indicates otherwise –

"Accounting Officer" means:

In a Municipality: The Municipal Manager

"Executive Authority" means:

In a Municipality: The Municipal Council

"Institutions" means:

Municipalities

"Risk Management Committee" means:

A committee appointed by the Accounting Officer, to review the Municipality's system of risk management

"Audit Committee" means:

An independent committee constituted to review the control, governance and risks management within the Institution, established in terms of section 66 of the MFMA.

"Chief Risk Officer" means:

A senior official within the organization responsible for risk management activities.

"Risk Management Unit" means:

A business unit responsible for coordinating and support the overall Institutional risk management process, but which does not assume the responsibilities of Management for identifying, assessing and managing risk.

"Chief Audit Executive" means:

A senior official within the organization responsible for internal audit activities.

"Internal Audit" means:

An independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance process.

"MFMA" means:

Municipal Finance Management Act (ACT No. 56 of 2003)

"King IV" means:

King IV™ is structured as a **Report that includes a Code**, with additional, separate sector supplements for SME's, NPO's, State-Owned Entities, Municipalities and Retirement Funds. The King Code™ contains both principles and recommended practices aimed at achieving governance outcomes.The King Code of Corporate Governance for South Africa 2016.

"Policy Framework" means:

Public Sector Risk Management Framework

"Risk" means:

Risk refers to an unwanted outcome, actual or potential, to the municipality's service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit.

"Risk Management" means:

Risk management is a systematic and formalised process instituted by the municipality to identify, assess, manage and monitor risks. Risk Management is proactive rather than reactive

"Enterprise Risk Management" means:

Enterprise Risk Management is a broad based application of risk management in all major functions and activities of the municipality, rather than in selected areas, to identify, assess, monitor and appropriately mitigate all material risks.

"Impact" means:

The result or effect on the Municipality's objectives should the risk materialise.

"Likelihood" means:

The probability that a risk will occur.

"Inherent Risk" means:

The risk to the Municipality in the absence of any actions management might take to alter either the risk's likelihood or impact.

"Residual Risk" means:

The remaining risk after management has taken action to alter the risk's likelihood or impact.

"Risk Appetite" means:

The amount of risk that the Municipality is willing to accept in pursuit of its mission or vision.

''Risk Intelligence'' means:

Improved business intelligence about the Municipality's internal and external environments and how prepared the Municipality is to prevent or quickly detect and correct potentially high impact areas.

"Risk Tolerance" means:

Acceptable variation relative to the achievement of an objective.

"Risk Owner**"** means:

The person accountable for managing a particular risk.

"Risk Champions" means:

A person who by virtue of his/her expertise or authority champion a particular aspect of the risk management process, but who is not the risk owner.

"Root cause" means:

Any threat or event which creates, or has the potential to create risk.

1.2 INTRODUCTION

(1) The Accounting Officer has committed **West Rand District Municipality** (WRDM) to a process of risk management that is aligned to the principles of good governance, as supported by the Municipal Finance Management Act (MFMA), Act no 56 of 2003.

(2) The concept of risk management is not new to the public service as the basic principles of service delivery (Batho Pele, 1997) clearly articulate the need for prudent risk management to underpin the achievement of government objectives.

(3) The public sector environment is fraught with unique challenges, such as lack of capacity, lengthy decision lead times, limited resources, competing objectives and infrastructure backlogs to mention a few.

(4) Such dynamics place an extra risk management burden on public sector managers to contain risks within acceptable limits.

(5) Risk management is a valuable management tool that increases the institutions prospects of success through getting it right the first time and minimising negative outcomes.

(6) Local and international trends confirm that risk management is a strategic imperative rather than an option within high performing institutions.

(7) High performing institutions set clear realistic objectives, develop appropriate strategies aligned to the objectives, understand the intrinsic risks associated therewith and direct resources towards managing such risks on the basis of cost benefit principles.

(8) Institutions must, in accordance with the previously mentioned prescripts, implement and maintain effective, efficient and transparent systems of risk management and internal control.

(9) The underlying intention of the enterprise risk management is that Institutions should through the risk management process achieve, among other things, the following outcomes needed to underpin and enhance performance:

   a) more efficient, reliable and cost effective delivery of services;
   b) more reliable decisions;
   c) innovation;
   d) minimised waste and fraud;
   e) prevention of fraud and corruption;
   f) better value for money through more efficient use of resources; and

g) Better outputs and outcomes through improved programme and project management.

1.2.1 Benefits of risk management

- **Increasing probability of achieving objectives -** As risk management is participatory and proactive, it helps management achieve the municipality's performance and financial targets and assists with the prevention of loss of resources. Controls and risk interventions will be chosen on the basis that they increase the likelihood that the municipality will fulfil its intentions / commitments to its stakeholders.
- **Aligning risk appetite and strategy-** Management considers their risk appetite in evaluating strategic alternatives, setting related objectives and developing mechanisms to manage related risks. Risk management thus assists management to take the right decisions in an uncertain environment. Focusing on risk analysis and responses improves the quality of strategic plans. It generates plans, which are comprehensive and analytical.
- **Enhancing risk response decisions-** Risk management provides the rigour for management to identify alternative risk responses – risk treatment, transfer, terminate and tolerate.
- **Reducing operational surprises and losses -** The municipality gains enhanced capability to identify potential events and establish responses thereby reducing surprises and associated costs or losses i.e. meeting targets and reducing over / under spending of the budget.
- **Identifying and managing multiple and cross enterprise risks -** Municipality face a myriad of risks affecting multiple parts. Risk management facilitates coordinated responses to the interrelated impacts and enhances an integrated response to multiple risks.
- **Seizing opportunities -** By considering a full range of potential events, management is positioned to identify and proactively realise opportunities.
- **Ensuring proper financial and asset management -** Risk management contributes to ensuring that there is proper financial and asset management within the municipality.
- **Ensuring compliance with laws and regulations -** Risk management contributes to effective reporting and monitoring of compliance with laws and regulations and assists with the limitation of damage to the municipality's reputation and associated consequences.

Seen in this context, it is clear why the Gauteng Provincial Government places a high importance on positioning risk management as a central part of service delivery improvement. Such importance is further emphasised with the various legislative instruments which make up the legal framework for risk management in the public sector.

The King Report on Governance in South Africa, 2016 (King IV) also places emphasis on integrating risk management into the organisations operations. ISO 31000 and COSO framework. The objective of the King IV report is p**romote corporate governance as integral to running an organisation and delivering governance outcomes** such as ethical culture, good performance, effective control and legitimacy.

The WRDM endorses endorse the adoption of this risk management framework as a fundamental step towards an outward looking, accountable and innovative public sector.

Yours sincerely,

____

Mr. ME Koloi

Acting Municipal Manager

West Rand District Municipality

Date: 8|12|21

SECTON 2 - PURPOSE AND BACKGROUND

2.1 PURPOSE

(1) To provide a comprehensive and consistent approach to the implementation of risk management;
(2) to provide guidance to the accounting officer, the executive council, managers and staff when overseeing or implementing the development of processes, systems and techniques for managing risk;
(3) to provide management with proven risk management tools that support their decision-making responsibilities and processes, together with managing risks, which impact on the objectives and key value drivers of the municipality;
(4) to support the objectives of municipality in enhancing their systems of risk management
(5) to protect against adverse outcomes and optimize opportunities; and
(6) to assist in embedding risk management process into the day to day activities of the municipality and integrating risk into institutional processes.

2.2 BACKROUND

(1) Risk management forms a critical part of any municipality's strategic management. It is the process whereby a municipality both methodically and intuitively addresses the risk attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of activities.
(2) Risk management is therefore recognized as an integral part of sound organizational management and is being promoted internationally and in South Africa as good practice applicable to the public and private sectors.
(3) The underlying premise of risk management is that every governmental body exists to provide value for its stakeholders.
(4) Such value is based on the quality of service delivery to the citizens. All municipality face uncertainty, and the challenge for management is to determine how much **uncertainty** the municipality is prepared to accept as it strives to grow stakeholder value.
(5) Uncertainty presents both risk and opportunity, with the potential to erode or enhance **value**.

2.2.1 Uncertainty

The Municipality operates in environments where factors such as technology, regulation, restructuring, changing service requirements and political influence create uncertainty.

Uncertainty emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes.

2.2.2 Value

Value is created, preserved or eroded by management decisions ranging from strategic planning to daily operations of the municipality. Inherent in decisions is the recognition of risk and opportunity, requiring that management consider information about the internal and external environment, deploys precious resources and appropriately adjusts municipal activities to changing circumstances. For municipality, value is realised when constituents recognize receipt of valued services at an acceptable cost. Risk management facilitates management's ability to both create sustainable value and communicate the value created to stakeholders.

The following factors require consideration when integrating risk management into municipal decision making structures:

- Aligning risk management with objectives at all levels of the municipality;
- Introducing risk management components into existing strategic planning and operational practices;
- Communicating municipal directions on an acceptable level of risk;
- Including risk management as part of employees' performance appraisals; and
- Continuously improving control and accountability systems and processes to take into account risk management and its results.

The ***Risk Management Policy*** **Framework** formally sets out the municipality's position on risk management and specifically addresses the structures and processes implemented to manage risks on an enterprise-wide basis in a consistent manner.

The ***Risk Management Implementation Plan*** facilitates the execution of risk management. The implementation plan gives effect to the risk management policy framework and sets out all the risk management activities planned for the financial year.

Current trends in good corporate governance have given special prominence to the process of risk management and reputable organisations are required to demonstrate that they comply with expected risk management standards. This means that the Municipality must ensure that the process of risk management receives special attention throughout the organisation and that ***all levels of management know, understand and comply with the framework document.***

SECTION 3 - LEGAL MANDATE

3.1 Accounting Officer

Section 62 (1) (c) (i) of the Municipal Finance Management Act (Act 56 of 2003) (MFMA) requires that:

"(1) The accounting officer of a municipality is responsible for managing the financial administration of the municipality, and must for this purpose take all responsible steps to ensure - (c) that the municipality has and maintains effective, efficient and transparent systems - (i) of financial and risk management and internal control."

3.2 Management

Section 78 of the Municipal Finance Management Act (Act 56 of 2003) (MFMA), states that, the extension of general responsibilities in terms of Section 78 of the MFMA to all senior managers and other officials of municipality implies that responsibility for risk management vests at all levels of management and that it is not limited to only the accounting officer and internal audit.

3.3 Internal Audit

Section 165 (2) (a), (b) (iv) of the Municipal Finance Management Act (Act 56 of 2003) (MFMA) states that:

"(2) The internal audit unit of a municipality or municipal entity must -

(a) prepare a risk based audit plan and an internal audit program for each financial year;

(b) advise the accounting officer and report to the audit committee on the implementation of the internal audit plan and matters relating to:

(iv) risk and risk management."

3.4 Audit Committee

Section 166 (2) (a) (ii) of the Municipal Finance Management Act (Act 56 of 2003) (MFMA) states that: *"(2) An audit committee is an independent advisory body which must – (a) advise the municipal council, the political office-bearers, the accounting officer and the management staff of the municipality, or the board of directors, the accounting officer and management staff of the municipal entity, on matters relating to (ii) risk management."*

SECTION 4 - RISK MANAGEMENT PROCESS

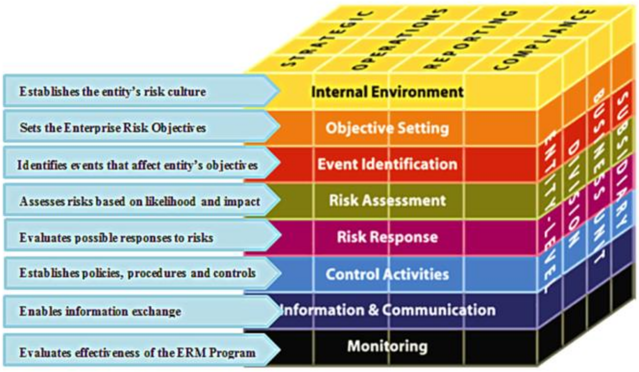
4.1 Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. These components are:

- ***Internal Environment*** – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- ***Objective Setting*** – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
- ***Event Identification*** – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are directed back to management's strategy or objective-setting processes.
- ***Risk Assessment*** – Risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- ***Risk Response*** – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- ***Control Activities*** – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- ***Information and Communication*** – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- ***Monitoring*** – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both. Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

4.2 Relationship of Objectives and Components

There is a direct relationship between objectives, which are what an organisation strives to achieve, and enterprise risk management components, which represent what is needed to achieve them.
The relationship is depicted in a three-dimensional matrix, in the form of a cube.



4.3 INTERNAL ENVIRONMENT

The municipality's internal environment is the foundation of risk management, providing discipline and structure. The internal environment influences how strategy and objectives are established, the municipality's activities are structured, and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems, and monitoring activities.

The internal environment comprises many elements, including the municipality's ethical values, competence and development of personnel, management's operating style and how it assigns authority and accountability.

As part of the internal environment management establishes the risk management philosophy, establishes the risk tolerance levels, inculcates a risk culture and integrates risk management with related initiatives.

The internal environment consists of different layers that should all be present and functioning. The layers are discussed in detail below:

4.3.1 Risk Management Philosophy – The risk management philosophy is the set of shared beliefs and attitudes that characterise how the municipality considers risk in everything it does from strategy development and implementation to its day to day activities. The risk management philosophy reflects the municipality's values, influencing its culture and operating style, and affects how the risk management components are applied, including how risks are identified, what risks are accepted and how they are managed.

The overall risk philosophy of the municipality is to identify, assess and manage its risks so as to preserve its strategic objectives and create value for all its stakeholders

4.3.2 Risk Appetite - The risk appetite can be defined as the amount of risk that the municipality is willing to accept in pursuit of its mission / vision.

The risk appetite guides resource allocation. Management allocates resources across functional areas with consideration of the municipality's risk appetite and units' plans for ensuring that objectives are met and expenditure remains within budget. Management considers its risk appetite as it aligns the municipality, its people and processes and designs the infrastructure necessary to effectively respond to and monitor risks.

The risk appetite enables an improved consistency of decision making at all levels through improving risk understanding and also provides a framework for knowingly taking risk within defined boundaries. The risk appetite derives real value from the assessment of risk over and above compliance purposes.

The risk appetite decided upon should be formally considered as part of the setting of strategy, with capital expenditure and other strategic decisions reviewed against it as they arise.

The key determinants of risk appetite are as follows:

- Expected performance;
- The capital needed to support risk taking;
- The culture of the municipality;
- Management experience along with risk and control management skills;
- Longer term strategic priorities;

The formulation of the risk appetite is typically closely aligned to the strategic planning process and is also inclusive of budgeting; as such it should be reviewed by management and the accounting officer on an annual basis.

4.3.3. Risk Tolerance - Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. Risk tolerances can be measured, and often are best measured in the same units as the related objectives. Performance measures are aligned to help ensure that actual results will be within the acceptable risk tolerances. In setting risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with risk appetite. Operating within risk tolerances provides management greater assurance that the municipality remains within its risk appetite and, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

4.3.4 Council - The municipality's Council is a critical part of the internal environment and significantly influences other internal environment elements.

4.3.*5* ***Integrity and Values*** - Management integrity is a prerequisite for ethical behaviour in all aspects of a municipality's activities. The effectiveness of risk management cannot rise above the integrity and ethical values of the people, who create, administer and monitor the municipality's activities.

Integrity and ethical values are essential elements of a municipality's internal environment affecting the design, administration and monitoring of components of the risk management process.

4.3.6 Commitment to competence - Competence reflects the knowledge and skills needed to perform assigned tasks. Management should decide how well these tasks need to be accomplished weighing the municipality's strategy and objectives against plans for strategy implementation and the achievement of objectives.

The competency levels for particular jobs should be specified and translated into requisite knowledge and skills. The necessary knowledge and skills in turn may depend on individuals training and experience. Factors considered in developing knowledge and skill levels include the nature and degree of judgement to be applied to a specific job.

4.3.7 Organisational structure - The municipality's organisational structure provides the framework to plan, execute, control and monitor its activities. A relevant organisational structure includes defining key areas of authority and responsibility and establishing the appropriate reporting lines
The organisational structure should be organised to enable effective risk management and to carry out its activities so as to achieve its objectives.
4.3.8 Authority and responsibility - This includes establishing the reporting relationships and authorisation protocols as well as policies that describe appropriate practices, knowledge and experience of key personnel as well as the resources for carrying out duties.

A critical challenge is to delegate to the extent required to achieve objectives, this means ensuring that decision making is based on sound practices for risk identification and assessment. Another challenge is ensuring that all personnel understand the municipality's objectives and how their actions interrelate and contribute to the achievement of the objectives.

4.3.9 Human resource policies and procedures - Human resource policies and practices pertaining to hiring, orientation, training, evaluating, counselling, and promoting, compensating and taking remedial actions send messages to employees regarding the expected levels of integrity, ethical behaviour and competence.

Furthermore it is essential that employees be equipped to tackle new challenges as risks throughout the municipality change and become more complex. Education and training must help employees to deal effectively with a changing environment.

4.4 OBJECTIVES SETTING

Objectives must exist before management can identify events potentially affecting their achievement. Risk management ensures that management has a process in place to both set objectives and align the objectives with the municipality's mission, vision, and organisational values and is consistent with the municipality's risk appetite and tolerance levels. The setting of these objectives is usually completed during the, "Strategic planning and Budgetary process."

The municipality's objectives can be viewed in the context of four categories:

Strategic – relating to high-level goals, aligned with and supporting the municipality's mission/vision;
Operations – relating to effectiveness and efficiency of the municipality's operations, including performance and service delivery goals. They vary based on management's choices about structure and performance;
Reporting – relating to the effectiveness of the municipality's reporting. They include internal and external reporting and may involve financial or non-financial information;
Compliance – relating to the municipality's compliance with applicable laws and regulations.

Having confirmed and clearly documented the municipality's objectives, it is necessary to identify all potential risks and threats relating to processes, assets and strategy. These are the possible problems and situations that may hinder the achievement of the objectives of the municipality.

4.5 RISK IDENTIFICATION

The risk identification phase is a deliberate and systematic effort to identify and document the municipality's key risks. The objective of risk identification is to understand what is at risk within the context of the municipality's objectives and to generate a comprehensive list of risks based on the threats and events that might prevent, degrade, delay or enhance the achievement of the objectives.

The municipality should adopt a rigorous and ongoing process of risk identification that also includes mechanisms to identify new and emerging risk timeously. The risk identification process should cover all risks, regardless of whether or not such risks are within the direct control of the municipality.

Risk workshops and interviews are useful for identification, filtering and screening risks but it is important that these judgment based techniques be supplemented by more robust and sophisticated methods where possible, including quantitative techniques.

Relevant and up to date information is important in identifying risks. Risk identification should be strengthened by supplementing management's perceptions of risk with:

- Review of external and internal audit reports;
- Financial analyses;
- Historic data analyses;
- Actual loss of data;
- Interrogation of trends in key performance indicators;
- Benchmarking against peer groups or quasi peer groups;
- Market and sector information;
- Scenario analyses; and
- Forecasting and stress testing.

To ensure comprehensiveness of risk identification the municipality should identify risks through considering both internal and external factors, through appropriate processes of:

4.5.1 Strategic risk identification

To identify risks emanating from the choices made by the municipality, specifically with regard to whether such choices weaken or strengthen the municipality's ability to execute its constitutional mandate:

- Strategic risk identification should precede the finalization of strategic choice to ensure that potential risk issues are factored into the decision making process for selecting the strategic options;
- Risks inherent to the selected strategic choice should be documented, assessed and managed through the normal functioning of the system of risk management; and
- Strategic risks should be formally reviewed concurrently with changes in strategy, or at least once a year to consider new and emerging risks.

4.5.2 Operational risk identification

To identify risks concerned with the municipality's operations:

- Operational risk identification seeks to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events;

- Operational risk identification should be an embedded continuous process to identify new and emerging risks and consider shifts in known risks through mechanisms such as management and committee meetings, environmental scanning, process reviews and the like; and
- Operational risk identification should be repeated when changes occur such as significant environmental or institutional changes, or at least once a year, to identify new and emerging risks.

4.5.3 Project risk identification

To identify risks inherent to particular projects:

- Project risk should be identified for all major projects, covering the whole lifecycle; and
- For long term projects, the project risk register should be reviewed at least once a year to identify new and emerging risks.

4.6 RISK ASSESSMENT

Risk assessment is a systematic process to quantify or qualify the level of risk associated with a specific threat or event. The main purpose of risk assessment is to help management to prioritise the identified risks. This enables management to spend more time, effort and resources to manage risks of higher priority than risks with a lower priority. The output of the risk assessment is a risk register enriched by the addition of ratings for each risk.

Risks should be assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence on the particular objective it is likely to affect. The risk assessment is performed using a 3 step process.

Step 1: Develop the scoring system for Impact and Likelihood before the actual assessment.

The following is a rating table that is utilised to assess the **Impact** of risks:

Rating	Impact	Definition
5	Critical	It is very unlikely that this objective will be achieved therefore there's 1 - 29% chances that this objective will be achieved.
4	Significant	It is unlikely that this objective will be achieved therefore there's 30 - 49% chances that this objective will be achieved.
3	Moderate	The objective maybe achieved therefore there are 50 - 69% chances that the objective will be achieved.

2	Minor	It is likely that this objective will be achieved therefore there are 70 - 89% chances that this objective will be achieved.
1	Low	The objective will certainly be achieved therefore there's 90 - 100% chances that the objective will be achieved.

The following is a rating table that is utilised to assess the **Likelihood** of risks:

Rating	Assessment	Definition
5	Almost certain	There's a 90-100% chance that this risk will definitely occur.
4	Likely	There's a 70 - 89% chance that this risk will occur.
3	Moderate	There's a 50 - 69% chance that this risk may occur.
2	Unlikely	There's a 30 - 49% chance that this risk will not occur.
1	Rare	There's a 1 - 29% chance that this risk will not occur in a long term.

Step 2: Apply the scores to the risk matrix to indicate what areas of the risk matrix would be regarded as high, medium or low risk.

Risk index = Impact x Likelihood

I	5	5	10	15	20	25
M	4	4	8	12	16	20
P	3	3	6	9	12	15
A	2	2	4	6	8	10
C	1	1	2	3	4	5
T		1	2	3	4	5
		LIKELIHOOD				

Risk index	**Risk Magnitude**
13 - 25	High
6 – 12	Medium
1 – 5	Low

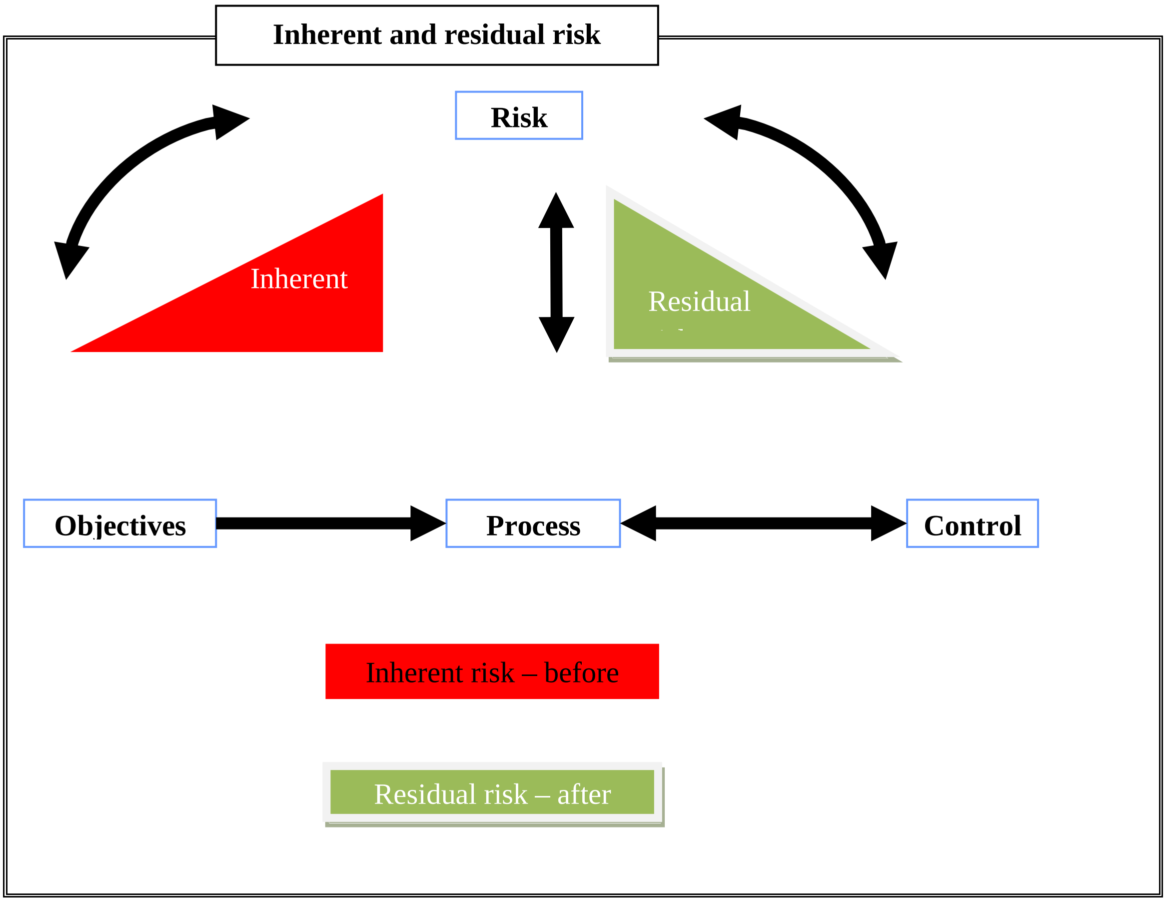
Step 3: Determine the acceptability of the risk and what action will be proposed to reduce the risk.

Risk index	Risk magnitude	Risk acceptability	Proposed actions
13 – 25	High risk	Unacceptable	Immediate implementation of corrective action plans.

6 –12	Medium risk	Acceptable with caution	Implementation of improvement opportunities and validation of controls.
1 - 5	Low risk	Acceptable	Validation and optimisation of controls.

Risk assessment is applied first to **inherent risk** – the risk to the municipality in the absence of any action management might take to alter either the risk's likelihood or impact. Then the **residual risk** is established to determine the actual level of risk after the mitigating effects of management actions to influence the risk.

The following diagram differentiates between inherent and residual risk.



4.7 RISK RESPONSE

Risk response is concerned with developing strategies to reduce or eliminate the threats and events that create risks. Risk response involves identifying and evaluating the range of possible options to address risks and implementing the chosen option.

Management should develop response strategies for all material risks, prioritising the risks exceeding or nearing the risk appetite level. Response strategies should be documented together with the responsibilities and timelines.

Risk responses fall within the following categories:

Category	Description
Treat	Manage the risk. Management undertakes to implement actions that are designed to reduce the likelihood, impact or both.
Transfer	Steps taken to shift the loss of liability to third parties such as insuring and outsourcing.
Terminate	Management takes action to remove the activities that gave rise to the risks.
Tolerate	Management accepts the risk. Informed decision to accept both the impact and likelihood of risk events.

4.8 CONTROL ACTIVITIES

Control activities are policies and procedures, which are the actions of people to implement the policies, directly or through application of technology, to help ensure that management's risk responses are carried out.
Control activities can be categorised based on the nature of the institution's objectives to which they relate: strategic, operations, reporting and compliance.
Although some control activities relate solely to one category, there often is overlap. Depending of circumstances, a particular control activity could help satisfy organisations objectives in more than of the categories. For example, certain operations controls can help ensure reliable reporting, reporting control activities can serve to effect compliance, and so on.

Management is responsible for designing, implementing and monitoring the effective functioning of system of internal controls. Approval, authorisation, segregation of duties, isolation of responsibility, access/custody/ (security), comparison and reconciliation, performance reviews. Without derogating from the above, everyone in the municipality should also have responsibilities for maintaining effective systems of internal controls, consistent with their delegated authority.

4.8.1 Integration with Risk Response

Having selected risk responses, management identifies control activities needed to help ensure that risk responses are carried out properly and in a timely manner.
Risk response serve as a focal point for the establishment of control activities. Control activities are built directly into the management process.
In selecting control activities, management considers how control activities are related to one another. In some instances, a single control activity addresses multiple risk responses. In other instances, multiple control activities are needed for the one risk response.
Management may find that existing control activities are sufficient to ensure that new risk response are executed effectively.
While control activities generally are established to ensure risk responses are appropriately carried out, with respect to certain objectives, control activities themselves are the risk response.

When selecting risk responses considers their appropriateness and remaining or residual risk, selection or review of control activities should include consideration of their relevance and appropriateness to the risk responses and related objectives.

Control activities are important part of the process by which a municipality strives to achieve its objectives. Control activities are not performed simply for their own sake or because it seems to be the “right or proper” thing to do.

4.8.2 Types of Control Activities

4.8.2.1 Policies and procedures

Control activities involve two key elements, namely, a policy establishing what should be done and procedures to effect the policy.
Policies must be implemented thoughtfully, conscientiously and consistently. Control activities serve as mechanisms for managing the achievement of set objectives. Control activities are actions, procedures supported by policies that help ensure that management responses are properly executed. They occur throughout the municipality, at all levels and in all functions.

4.8.2.2 Control over Information Systems

With widespread reliance on information systems to operate an organisation and meet reporting and compliance objectives, controls are needed over significant systems.

Two broad groupings of information systems control activities can be used. The first is general controls, which apply to many if not all application systems and help ensure their continued, proper operation.
The second is application controls, which include computerised steps within application software to control the processing. General and application controls, combined with manual process controls where necessary, work together to ensure completeness, accuracy, and validity of information.

4.8.2.3 General Controls

General controls include controls over information technology management, information technology infrastructure, security management, software acquisition, development, and maintenance. General controls apply to all systems – from mainframe to client/server to desktop and portable computer environments.

4.8.2.4 Application Controls

Application controls focus directly on completeness, accuracy, authorisation, and validity of data capture and processing. They help ensure data are captured or generated when needed, supporting applications are available, and interface errors are detected quickly and dealt with immediately.
An important objective of application controls is to prevent errors from entering the system, as well as to detect and correct errors once they are present.
To do this application controls often involve computerized edit checks consisting of format, existence, reasonableness, and other data checks built into applications during development. When properly designed, they can provide control over data entering the system.

4.8.3 Management should develop the internal control architecture through:

(a) Preventative controls to prevent errors or irregularities from occurring e.g. physical security of assets to prevent theft; and
(b) Detective controls to find errors or irregularities after they have occurred e.g. performance of reconciliation procedure to identify errors.

4.8.4 The internal control architecture should include:

(a) Management controls to ensure that the municipality's structure and systems support its policies, plans and objectives, and that it operates within laws and regulations;

(b) Administrative controls to ensure that policies and objectives are implemented in an efficient and effective manner;
(c) Accounting controls to ensure that resources are accounted for fully and transparently and are properly documented; and
(d) Information technology controls to ensure security, integrity and availability of information.

4.9 INFORMATION AND COMMUNICATION

Pertinent information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems use internally generated data, and information from external sources, providing information for managing risks and making informed decisions relative to objectives.
Effective communication also occurs, flowing down, across and up the organisation. All personnel receive a clear message from top management that enterprise risk management responsibilities must be taken seriously.

4.9.1 Information

Information is needed at all levels of an organisation to identify, assess, and respond to risks, and to otherwise run the organisation and achieve its objectives.
Operating information form internal and external sources, both financial and non-financial, is relevant to multiple business objectives. Financial information, for instance, is used in developing financial statements for reporting purposes, and also for operating decisions, such as monitoring performance and allocation of resources. Reliable information is fundamental to planning, budgeting, performance evaluation and a range of other management activities.

4.9.2 Information Quality

With increasing dependence on sophisticated information systems and data-driven automated decision systems and processes, data reliability is crucial. Inaccurate data can result in unidentified risks or poor assessments and bad management decisions.

The quality of information includes ascertaining whether:

- Content is appropriate – Is it at the right level of detail?
- Information is timely – Is it there when required?
- Information is current – Is it the latest available?
- Information is accurate – Is the data correct?
- Information is accessible - Is it easy to obtain by those who need it?

Having the right information, on time and at the right place, is essential to effecting enterprise risk management. Hence information systems, while a component of enterprise risk management, also must be controlled.

4.9.3 Communication

Communication is inherent in information systems. As discussed above, information systems must provide information to appropriate personnel to enable them to carry out their operating, reporting and compliance responsibilities. But communication also must take place in a broader sense, dealing with expectations, responsibilities of individuals and groups, and other important matters.

4.9.3.1 Internal

Management provides specific and directed communication that addresses behavioural expectations and the responsibilities of personnel. This includes a clear statement of the organisation's risk management philosophy and approach and a clear delegation of authority. Communication about processes should align with, and underpin, the desired culture.

All personnel across the organisation, need to receive a clear message from top management that enterprise risk management must be taken seriously. Both the clarity of the message and effectiveness with it is communicated are important. Personnel also

Relevant information, properly and communicated is essential to equip the relevant officials to identify and assess and respond to risks.

Effective information and communication is intended to support and enhanced decision making and accountability through:

- Relevant, timely, accurate and complete information;
- Communicating responsibilities and actions.

4.10 MONITORING

4.10.1 Risk monitoring

(1) Monitoring concerns checking on a regular basis to confirm the proper functioning of the entire risk management system.

(2) Monitoring should be effected through ongoing activities or separate evaluations to ascertain whether risk management is effectively practiced at all levels and across the Institution in accordance with the risk management policy, strategy and plan.

Monitoring activities should focus on:

- **Monitoring of risk action plans** - Risk action plans need to be monitored on an ongoing basis to ensure the necessary actions are implemented on schedule and as intended.
- **Monitoring of controls** - The effective operation of existing controls as well as their cost effectiveness needs to be evaluated regularly. Evaluations may include management reviews, self assessment reviews and third party reviews as appropriate. Internal audit should also perform periodic reviews on existing controls as well as the implementation of necessary additional controls on a periodic basis.
- **Monitoring of new and emerging risks** - The risk profile of any organisation will change over time. Thus there is a need to monitor and review the risk profile of the municipality to ensure that it remains relevant and complete. Changes in strategy, the legal and regulatory environment, restructuring, loss of key personnel, significant control deficiencies, fraud, changes in business objectives will require an immediate review of municipal risk profiles.
- **Monitoring of the effectiveness of the risk management process** - The efficiency of the entire risk management process should be monitored periodically. A positive correlation should exist between improvements in the system of risk management as well as institutional performance.

4.10.2 Incident reporting

Incident reporting is another means of risk monitoring and reviewing the effectiveness of controls. Certain disciplines such as Safety, Health, Environmental and Quality may already have in place incident reporting systems. Such reporting systems should be integrated into the broader risk management incident reporting systems in order to avoid duplication of effort.

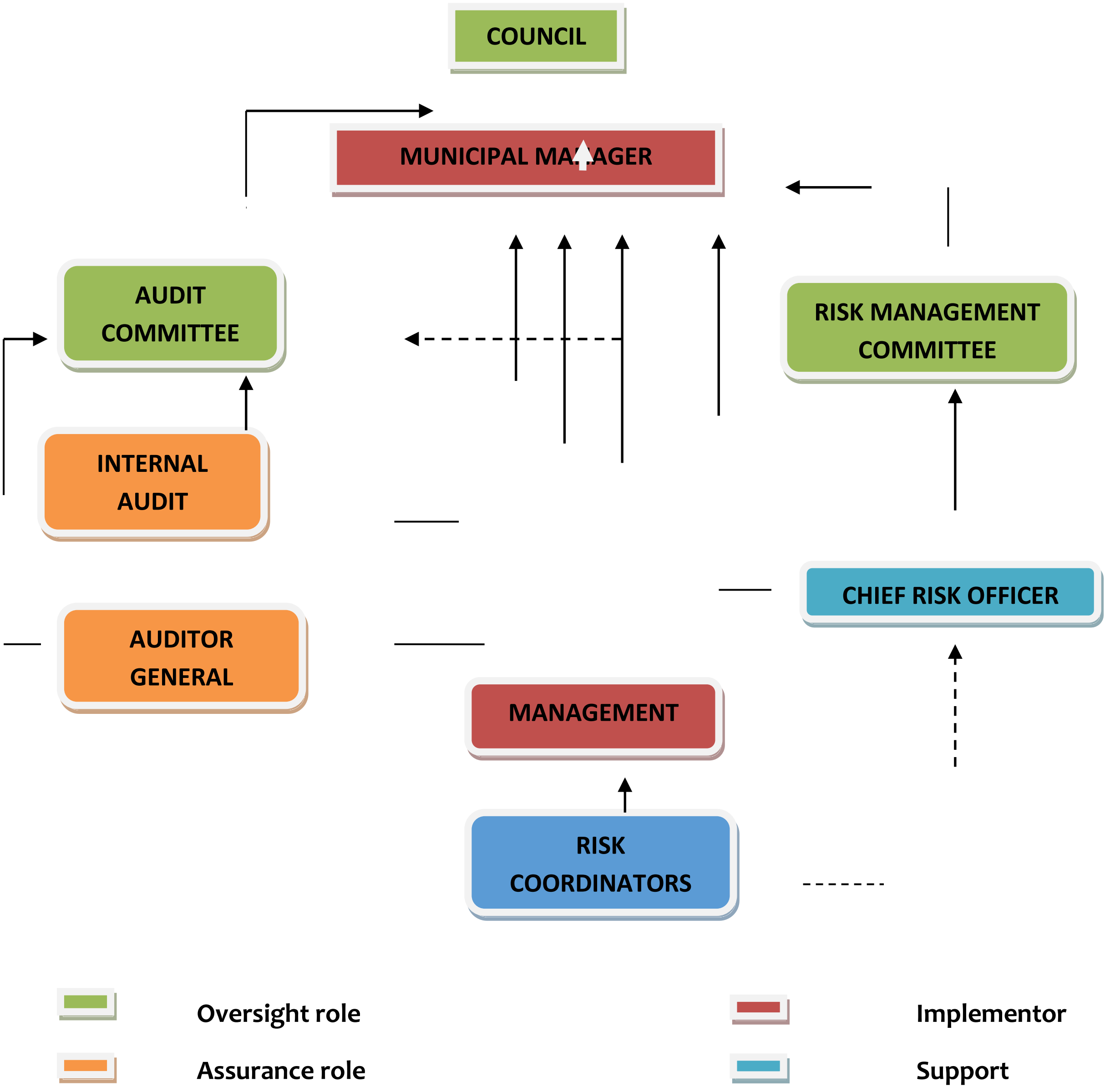
4.10.3 Performance measurement

Management's performance with the processes of risk management will be measured and monitored through the following performance management activities:

- Monitoring of progress made by management with the implementation of the risk management framework;
- Monitoring of loss and incident data;
- Management's progress made with risk mitigation action plans; and
- An annual quality assurance review of risk management performance.

SECTION 5 ROLES AND RESPONSIBILITIES

The parties that have a significant role to play in the process of risk management are set out below:



5.1 Executive Council

The executive authority should take an interest in risk management to the extent necessary to obtain comfort that properly established and functioning systems of risk management are in place to protect the municipality against significant risks.

Responsibilities of the Council Authority include:

- Ensuring that the institutional strategies are aligned to the Government mandate;
- Obtaining assurance that the municipality's strategic choices were based on a rigorous assessment of risk;
- Obtaining assurance from management that key risks inherent in the municipality's strategies were identified and assessed and are being properly managed;
- Assisting the accounting officer to deal with fiscal, intergovernmental, political and other risks beyond their direct control and influence; and
- Insisting on the achievement of objectives, effective performance management and value for money.
- Approves the risk management policy, framework and implementation plan.
- Approve the Fraud Prevention policy, strategy and implementation.

5.2 Accounting Officer

The accounting officer is the ultimate Chief Risk Officer (CRO) of the Municipality and is accountable for the municipality's risks.

More specifically, the high-level responsibilities of the accounting officer include:

- Setting an appropriate tone by supporting and being seen to be supporting the municipality's aspirations for effective management of risks.
- Delegating responsibilities for risk management to management and internal formations such as the risk management committee.
- Holding management accountable for designing, implementing, and monitoring and integrating risk management into their day to day activities.

- Holding the risk management committee accountable for performance in terms of its risk management responsibilities.
- Providing leadership and guidance to enable management and the risk management committee to properly perform their functions.
- Ensuring the control environment supports the effective functioning of risk management.
- Approving the municipality's risk appetite and tolerance level.
- Devoting personal attention to overseeing the management of significant risks.
- Leveraging the audit committee, internal audit, external audit and the risk management committee for assurance on the effectiveness of risk management.
- Ensuring that appropriate action in respect of the recommendations of the audit committee, internal audit, external audit and the risk management committee to improve risk management.
- Providing assurance to relevant stakeholders that key risks are properly identified, assessed and mitigated.

5.3 Risk Management Committee

The risk management committee is responsible for assisting the accounting officer in addressing the oversight requirements of risk management and evaluating and monitoring the municipality's performance with regards to risk management.

- Review the risk management policy, framework, risk management implementation plan and recommend for approval by the executive authority.
- Review the fraud prevention policy, strategy and implementation plan and recommend for approval by the accounting officer.
- Review the risk appetite and tolerance and recommend for approval by the accounting officer.
- Review the municipality's risk identification and assessment methodologies to evaluate their effectiveness in timeously and accurately identifying the municipality's risks.
- Monitor and assess the implementation of the risk management policy, framework and implementation plan.
- Monitoring the reporting of risk by management with particular emphasis on significant risks or exposures and appropriates of the steps management has taken to reduce the risks to an acceptable level.
- Review the material findings and recommendations by assurance providers on the system of risk management and monitor the implementation of such recommendations.

- Develop its own key performance indicators for approval by the accounting officer.
- Interact with audit committee to share information relating to material risks of the municipality.
- Provide timely and useful reports to the accounting officer on the state of risk management, together with recommendations to address any deficiencies identified by the committee.
- Reviewing the impact of any changes in the municipality on the risk management process and response to these changes including the update of the risk profile.

5.4 Audit Committee

The audit committee is an independent committee responsible for oversight of the municipality's control, governance and risk management. The responsibilities of the audit committee should be clearly defined in its charter.

5.4.1 The responsibilities of the audit committee include:

- The audit committee should provide an independent and objective view of the Municipality's risk management effectiveness;
- Reviewing and recommending disclosures on matters of risk and risk management in the annual report;
- Providing feedback to the accounting officer on the adequacy and effectiveness of risk management in the municipality, including recommendations for improvement;
- Ensure the acceptability of the risk profile in conjunction with the overall risk appetite of the municipality, taking into account all risk mitigation factors including but not limited to internal controls, business continuity and disaster recovery planning, etc.
- Ensuring that the internal and external audit plans are aligned to the risk profile of the Municipality;
- Satisfying itself that it has appropriately addressed:
    - i Financial reporting risks, including the risk of fraud;
    - ii Internal financial controls;
    - iii IT risks as they relate to financial reporting.
- The audit committee should evaluate the effectiveness of internal audit in its responsibilities for risk management.

5.5 Chief Risk Officer

The chief risk officer provides specialist expertise in providing a comprehensive support service to ensure systematic, uniform and effective risk management in the municipality.

5.5.1 The specific roles and responsibilities include:

- Working with senior management to develop the municipality's vision for risk management.
- Developing, in consultation with management, the municipality's risk management framework, risk management policy, risk management implementation plan as well as risk appetite and tolerance levels for approval by the accounting officer;
- Communicating the risk management policy, risk management framework and risk management implementation plan to all stakeholders in the municipality and monitoring its implementation;
- Continuously driving the risk management process towards higher levels of maturity;
- Developing a common risk assessment methodology that is aligned with the municipality's objectives at strategic, tactical and operational levels for approval by the Accounting Authority / Officer.
- Assisting management with risk identification, assessment and the development of response strategies;
- Monitoring the implementation of response strategies;
- Collating, aggregating, interpreting and analysing the results of risk assessments to extract risk intelligence;
- Reporting risk intelligence to the accounting officer, management and the risk management committee;
- Participating with internal audit, management and the auditor - general in the development of the assurance plan;
- Ensuring effective information systems exist to facilitate overall risk management improvement within the municipality;
- Continuously transferring risk management principles and practices, through training interventions, to all stakeholders within the municipality;
- Coordinate reporting on actual non compliance incidents and losses incurred;
- Communicates with the audit committee and the risk management committee on the status of risk management;
- Providing input into the development and subsequent review of the fraud prevention strategy, business continuity plans occupational health, safety and environmental policies and practices and disaster management plans.

5.6 Internal Audit

Internal audit provides independent, objective assurance on the effectiveness of the risk management process.The specific roles and responsibilities include:

- Internal audit must evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary;
- In terms of the International Standards for the Professional practice of internal audit, determining whether risk management processes are effective is a judgement resulting from the internal auditors assessment that:
    - i Municipality objectives support and align with the municipality’s mission;
    - ii Significant risks are identified and assessed;
    - iii Risk responses are appropriate to limit risk to an acceptable level; and
    - iv Relevant risk information is captured and communicated in a timely manner to enable the accounting officer, management and the Risk Management Committee and other officials to carry out their responsibilities.
- Internal Audit must develop its internal audit plan on the basis of the key risk areas.

5.7 External Audit

The external auditor (Auditor - General) provides an independent opinion on the effectiveness of risk management.In providing an opinion the auditor - general focuses on:

- Determining whether the risk management policy, framework and implementation plan are in place and appropriate;
- Assessing the implementation of the risk management policy, framework and the implementation plan;
- Reviewing the risk assessment process to determine if it is sufficiently robust to facilitate timely and accurate risk rating and prioritisation; and
- Determining whether management action plans to mitigate the key risks are appropriate and are being effectively implemented.

5.8 Management

- Management is accountable to the accounting officer for designing, implementing and monitoring risk management, and integrating it into the day-to-day activities of the municipality.

- This needs to be done in such a manner as to ensure that risk management becomes a valuable strategic management tool for underpinning the efficacy of service delivery and value for money.

5.8.1 High level responsibilities of management include:

- Empowering officials to perform adequately in terms of risk management responsibilities through proper communication of responsibilities, comprehensive orientation and ongoing opportunities for skills development;
- Aligning the functional risk management methodologies and processes with the Municipality's processes;
- Providing risk management reports;
- Presenting to the risk management and audit committees as requested;
- Maintaining the proper functioning of the control environment within their area of responsibility;
- Holding officials accountable for their specific risk management responsibilities;
- Maintains a harmonious working relationship with the CRO and supports the CRO in matters concerning the functions of risk management;
- Keeps key functional risks at the forefront of the management agenda and devotes personal attention in overseeing the management of these risks.

5.9 Other Officials

- All other officials are responsible for integrating risk management into their day to day activities**.**

5.9.1 Responsibilities include:

- Applying the risk management processes to their respective functions;
- Implementing the delegated action plans to address the identified risks;
- Informing their supervisors and/ or the risk management unit of new risks and significant changes in known risks and
- Cooperating with other role players in the risk management process and providing information as required.

5.10 Risk Management Champions

- Risk management champion are drawn from the existing resources, from within the operations and functions of the various business units.

5.10.1 Responsibilities include:

- Coordinate risk management activities within functional areas in the municipality;
- Assist in embedding risk management within the municipality;
- Arrange and facilitate risk meetings, presentations and workshops involving staff within the functional area;
- Providing risk management training and development where required;
- Assist in collating and reporting on risk information;
- Provide guidance on matters relating to risk management.

SECTION 6 THE OUTPUTS OF RISK ASSESSMENTS ARE USED TO DIRECT INTERNAL AUDIT PLANS.

- Internal audit plans depend greatly on the outputs of risk assessments. Risks from risk assessments must be incorporated into internal audit plans according to management and audit committee priorities.
- The risk assessment process is useful for internal audit staff, because it provides the necessary priorities regarding risk as opposed to using standardised audit sheets.
- The audit activities will focus on adherence to controls for the key risks that have been identified. In addition, internal audit staff may direct management towards the need for better controls around key risks.

SECTION 7 THE GAUTENG DEPARTMENT OF FINANCE IS RESPONSIBLE FOR MONITORING AND ASSESSING THE IMPLEMENTATION OF RISK MANAGEMENT IN THE PROVINCE.

- A formal risk management process review will be conducted by the Department of Finance on a quarterly basis to assess the implementation of risk management in Municipality.

SECTION 8 SAFETY, HEALTH AND ENVIRONMENT

- A formal safety management programme is essential for Municipality.
- The scope of the safety management programme should include administrative aspects, safety awareness and training, health, hygiene, electrical safety, physical safety, micro-environmental exposures and legislative requirements.

SECTION 9 COMPLIANCE

- Compliance is a key element of the risk management process. All statutory compliance obligations must be managed to a minimum level.

SECTION 10 BUSINESS CONTINUITY MANAGEMENT

- It is expected that Municipality should have a Business Continuity Management Plan in place, which will be revised and tested at least annually.
- The results of such testing and simulations should be reported to the Risk Management Committee.

SECTION 11 FRAUD PREVENTION

- Each Municipality is responsible for the establishment of its own fraud prevention policy and plan.
- Confidential reporting of potential bridges and actual investigations should be reported to the Risk Management Committee.

SECTION 12 - ANNEXURE

12.1 Annexure A: Risk Categories

- As the risk environment is so varied and complex it is useful to group potential events into categories.
- By aggregating events horizontally across a municipality vertically within operating units, management develops an understanding of the interrelationships between events, gaining enhanced information as a basis for risk assessment.

The main categories to group individual risk exposures are as follows:

Risk type	Risk category	Description
Internal	Human resources	Risks that relate to human resources of an institution. These risks can have an effect on an institution's human capital with regard to: • Integrity and honesty; • Recruitment; • Skills and competence; • Employee wellness; • Employee relations; • Retention; and • Occupational health and safety.
	Knowledge and Information management	Risks relating to an institution's management of knowledge and information. In identifying the risks consider the following aspects related to knowledge management: • Availability of information; • Stability of the information; • Integrity of information data; • Relevance of the information; • Retention; and • Safeguarding.

	Litigation	Risks that the institution might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from: • Claims by employees, the public, service providers and other third party • Failure by an institution to exercise certain rights that are to its advantage.
	Loss \ theft of assets	Risks that an institution might suffer losses due to either theft or loss of an asset of the institution.
	Material resources (procurement risk)	Risks relating to an institution's material resources. Possible aspects to consider include: • Availability of material; • Costs and means of acquiring \ procuring resources; and • The wastage of material resources.
	Service delivery	Every institution exists to provide value for its stakeholders. The risk will arise if the appropriate quality of service is not delivered to the citizens.
	Information Technology	The risks relating specifically to the institution's IT objectives, infrastructure requirement, etc. Possible considerations could include the following when identifying applicable risks: • Security concerns; • Technology availability (uptime); • Applicability of IT infrastructure; • Integration / interface of the systems; • Effectiveness of technology; and • Obsolescence of technology.
	Third party performance	Risks related to an institution's dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with an institution. Non performance could include: • Outright failure to perform; • Not rendering the required service in time; • Not rendering the correct service; and • Inadequate / poor quality of performance.

	Health & Safety	Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within the institution.
	Disaster recovery / business continuity	Risks related to an institution's preparedness or absence thereto to disasters that could impact the normal functioning of the institution e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include: • Disaster management procedures; and • Contingency planning.
	Compliance \ Regulatory	Risks related to the compliance requirements that an institution has to meet. Aspects to consider in this regard are: • Failure to monitor or enforce compliance; • Monitoring and enforcement mechanisms; • Consequences of non compliance; and • Fines and penalties paid.
	Fraud and corruption	These risks relate to illegal or improper acts by employees resulting in a loss of the institution's assets or resources.
	Financial	Risks encompassing the entire scope of general financial management. Potential factors to consider include: • Cash flow adequacy and management thereof; • Financial losses; • Wasteful expenditure; • Budget allocations; • Financial statement integrity; • Revenue collection; and • Increasing operational expenditure.
	Cultural	Risks relating to an institution's overall culture and control environment. The various factors related to organisational culture include: • Communication channels and the effectiveness; • Cultural integration; • Entrenchment of ethics and values; • Goal alignment; and • Management style.

	Reputation	Factors that could result in the tarnishing of an institution's reputation, public perception and image.
External	Economic Environment	Risks related to the institution's economic environment. Factors to consider include: • Inflation; • Foreign exchange fluctuations; and • Interest rates.
	Political environment	Risks emanating from political factors and decisions that have an impact on the institution's mandate and operations. Possible factors to consider include: • Political unrest; • Local, Provincial and National elections; and • Changes in office bearers.
	Social environment	Risks related to the institution's social environment. Possible factors to consider include: • Unemployment; and • Migration of workers.
	Natural environment	Risks relating to the institution's natural environment and its impact on normal operations. Consider factors such as: • Depletion of natural resources; • Environmental degradation; • Spillage; and • Pollution.
	Technological environment	Risks emanating from the effects of advancements and changes in technology.
	Legislative environment	Risks related to the institutions legislative environment e.g. changes in legislation, conflicting legislation.